September 27, 2012 (Backgrounder – Prepared by Committee Staff)

Medical Devices: FDA Should Expand its Consideration of Information Security for Certain Types of Devices *(GAO 12-816)*

Rep. Donna F. Edwards, Ranking Member, Subcommittee on Technology and Innovation, Committee on Science, Space and Technology, **Rep. Edward J. Markey**, Ranking Member of the Committee on Natural Resources, and **Rep. Anna G. Eshoo**, Ranking Member of the Subcommittee on Communications and Technology and Co-chair of the House Medical Technology Caucus, requested a GAO report on the information security of implantable wireless medical devices. They requested the report after computer security experts demonstrated that certain devices could be intentionally breached by hackers.

BACKGROUND

Today, more than 25 million Americans rely on implantable medical devices and this number is expected to grow rapidly in the next few years. These devices include deep brain stimulators to help alleviate epileptic seizures, cardiac defibrillators, which use electricity to control irregular heartbeats, and insulin pumps that dispense insulin to diabetics. These devices have saved lives and improved the health of millions. However, since 2008 there have been at least four separate laboratory demonstrations showing wireless medical devices can be intentionally manipulated without proper authorization.

The Food and Drug Administration (FDA) is responsible for approving and ensuring the safety and effectiveness of all medical devices. According to the GAO, the FDA did not consider intentional information security risks as a realistic possibility until recently. Additionally, although the agency intends to reassess its approach to reviewing software used in medical devices, it does not plan to specifically address information security as part of this effort.

Manufacturers of these devices have also been exceedingly slow to publicly acknowledge these potential computer security risks. Manufacturers are required to include information about known defects in their devices in published material. However, the GAO found that the manufacturers of the two devices that were intentionally manipulated in the laboratory, a cardiac defibrillator and insulin pump, both failed to include information about known security vulnerabilities in their corporate annual reports and other publications.

RECOMMENDATIONS

The GAO recommends that the FDA develop and implement a more comprehensive plan to enhance its review and oversight of medical devices that more fully addresses the information security risks of these devices. The GAO listed four minimum actions the FDA should include in this plan:

1. Increase its focus on manufacturers' identification of potential unintentional and intentional computer security threats and vulnerabilities and strategies to mitigate these risks during its pre-market approval review process;

2. Utilize available resources, including those from other entities, such as other federal agencies, particularly the National Institute of Standards and Technology (NIST);

3. Leverage its post-market efforts to identify information security problems; and

4. Establish a specific schedule for completing this review and implementing these changes.